

MULTI-STEP DIGITAL SIGNATURE METHOD AND SYSTEM

Publication number: WO9639765 (A1)

Publication date: 1996-12-12

Inventor(s): SUDIA FRANK W [US]; FREUND PETER C [US]; HUANG STUART T F [US]

Applicant(s): BANKERS TRUST CO [US]; SUDIA FRANK W [US]; FREUND PETER C [US]; HUANG STUART T F [US]

Classification:

- international: G06Q20/00; G09C1/00; H04L9/08; H04L9/32; G06F7/72; G06Q20/00; G09C1/00; H04L9/08; H04L9/32; G06F7/60; (IPC1-7): H04L9/30; H04L9/32

- European: G06F21/00N5A2Q; G06F21/00N9C; G06Q20/00K1; H04L9/08S; H04L9/32; H04L9/32S3

Application number: WO1996US05317 19960419

Priority number(s): US19950462430 19950605

Also published as:

US5867578 (A)

ZA9603635 (A)

NZ306846 (A)

MX9709760 (A)

JP2006333520 (A)

more >>

Cited documents:

US5276737 (A)

US5481613 (A)

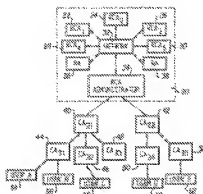
US5005200 (A)

US5224163 (A)

US5164988 (A)

Abstract of WO 9639765 (A1)

A multi-step signing system and method uses multiple signing devices (11, 13, 15, 17, 19) to affix a single signature which can be verified using a single public verification key. Each signing device possesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents (23, 25, 27, 29, 31). In a serial embodiment, after a first partial signature has been affixed, a second signing device exponentiates the first partial signature. In a parallel embodiment, each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature. Security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices and by distributing authority to affix a partial signature among a plurality of authorizing agents.



Data supplied from the **espacenet** database — Worldwide